RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART4-W02

The Next Chapter: AI, Modern Threats, and the Future of Cybersecurity

Peter Bailey
VP, Google Cloud Security

David Wong
Director, Mandiant Consulting, Google

Google Cloud

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

By the Numbers

M-Trends 2025 Report

Popular investigation stats

These metrics are based on Mandiant Consulting incident response investigations conducted January 1, 2024 – December 31, 2024.

11 days
global median dwell time

57%
external incident notifications

Exploits
most common initial infection vector

11 days
ransomware median dwell time

55%
attackers motivated by financial gain

Financial services
most targeted industry

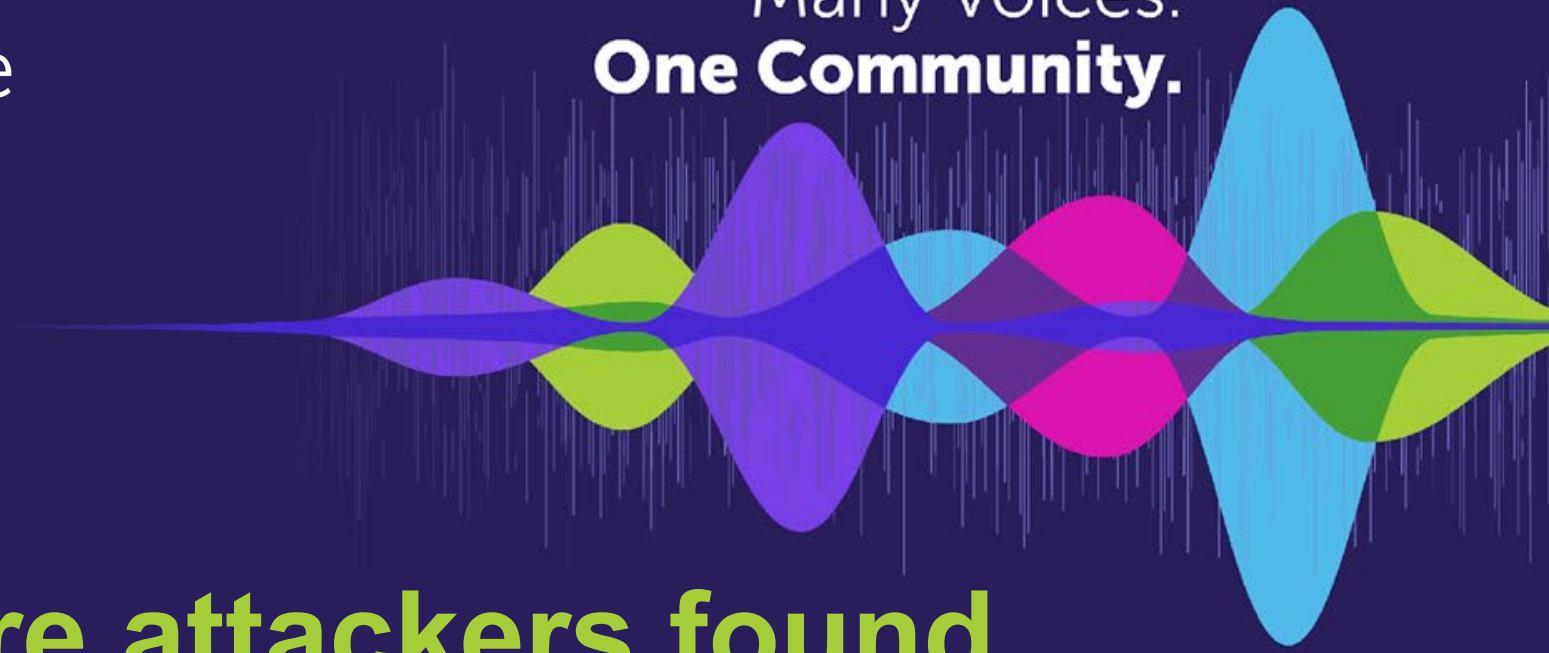
632
newly tracked malware families

71%
MITRE ATT&CK techniques used

Backdoors
most used malware category

RSAC 2025 Conference

Many Voices. One Community.



When are attackers found

Dwell time

Global median dwell time

Adversary notifications originate from extortion actors who benefit from monetizing intrusions quickly.

Median Dwell Time in days, 2011 - 2024

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
All	416	243	229	205	146	99	101	78	56	24	21	16	10	11

Median Dwell Time by Detection Source, 2024

	2024
All	11
Adversary	5
External Entity	26
Internal	10

RSAC 2025 Conference

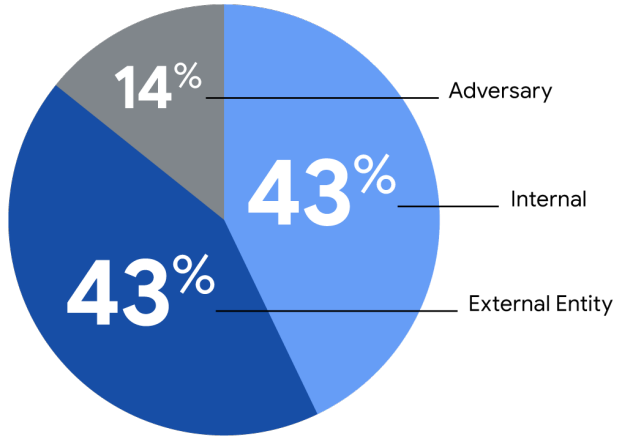
Many Voices. One Community.

How we find attackers

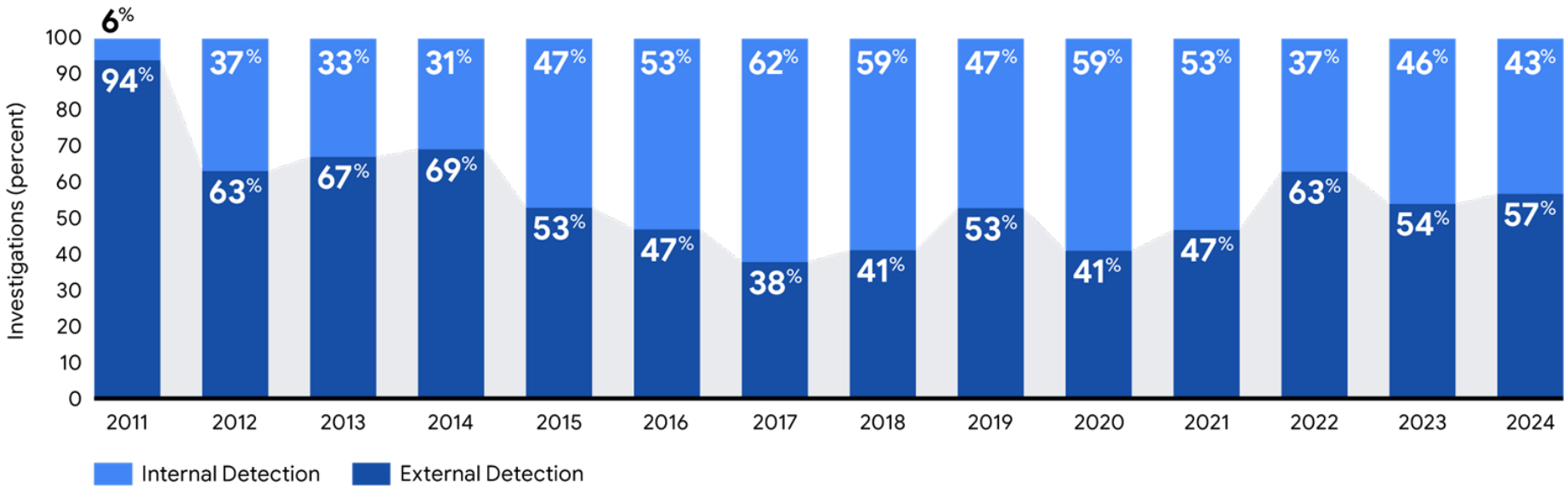
Detection source

Detection by Source

Adversary notifications typically take the form of ransom notes.

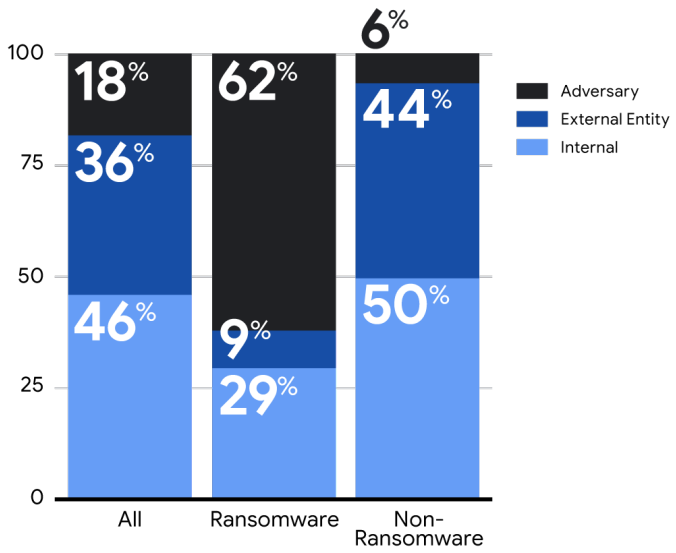


Global Detection by Source, 2011 -2024

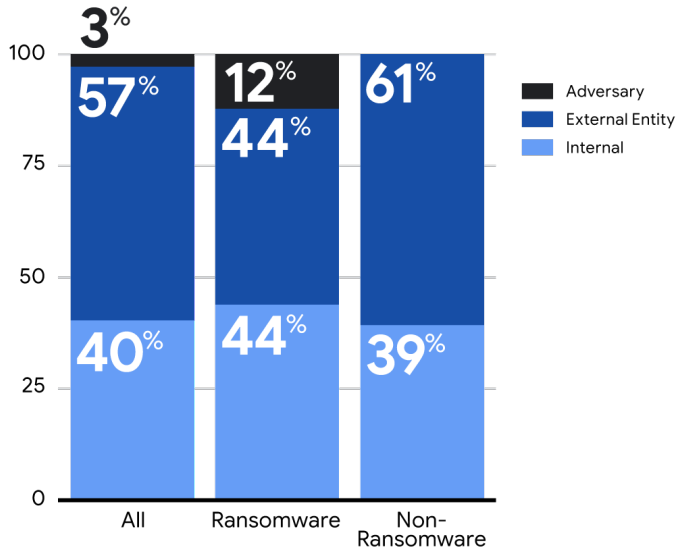


Detection by Source
Regional Reports

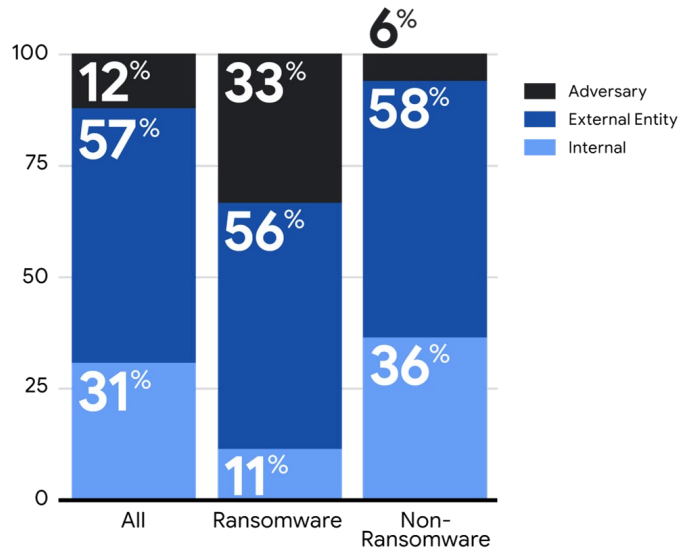
Americas Detection by Source, 2024



EMEA Detection by Source, 2024



JAPAC Detection by Source, 2024



AI Powered Threat Hunting

We pioneered an AI powered threat hunting model, the **Joint Investigation and Mitigation Initiative (JIMI),** to process election-focused collections.

20,000 **Individual domains** processed with 4,690 identified for human review

77% **Reduction in workload** saving 766 hours of analyst time

49 **Investigative leads** identified that would have otherwise not been discovered

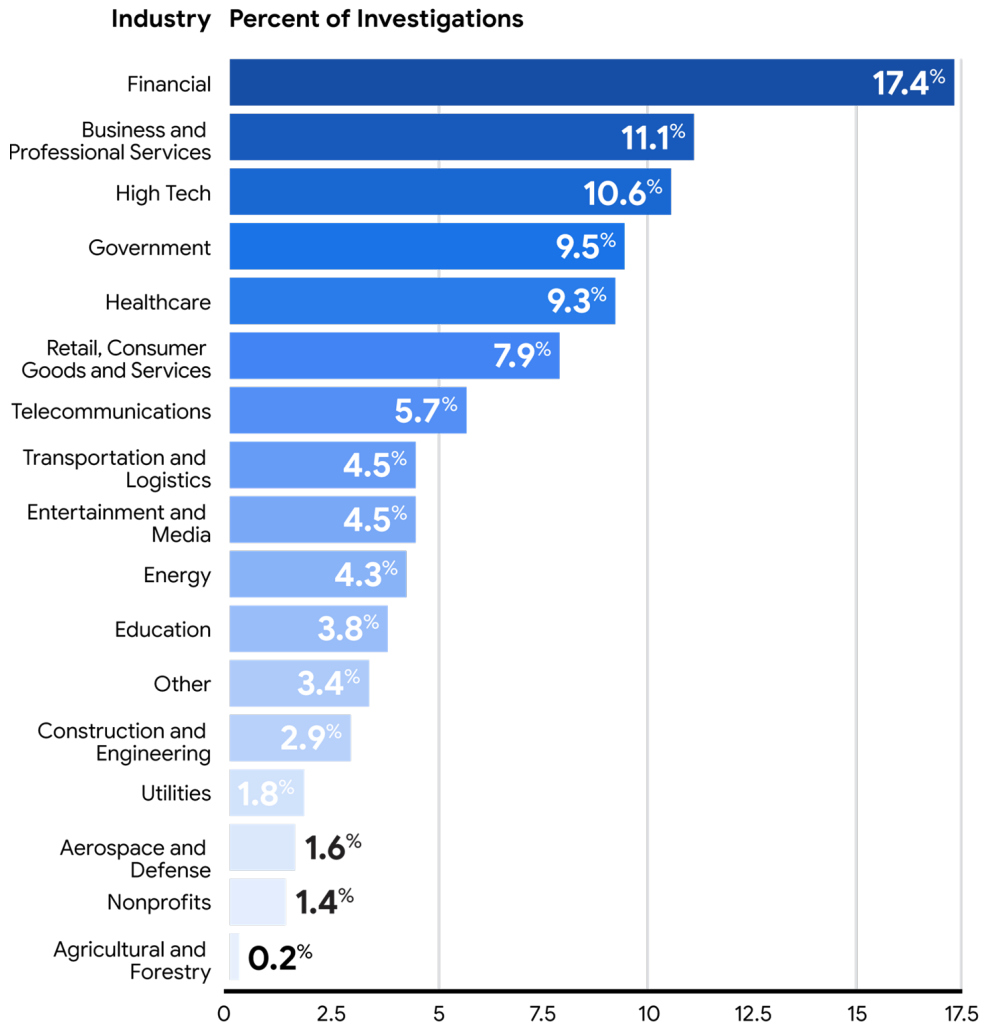
RSAC 2025 Conference

Many Voices. One Community.

What attackers target

Top industries and mission objectives

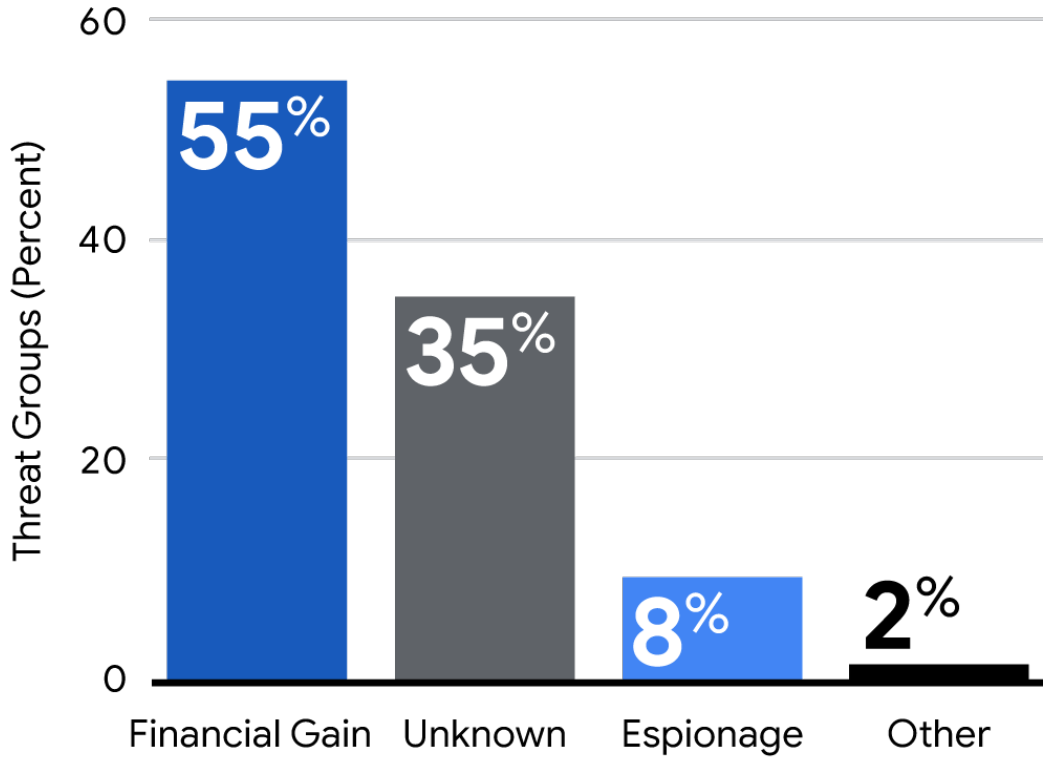
Targeted Industries



Observed Threat Groups by Goal

The growing share of financially motivated threat groups is likely due, in part, to the overall growth of impactful extortion intrusions.

Observed Threat Groups by Goal, 2024



RSAC 2025 Conference

Many Voices. One Community.

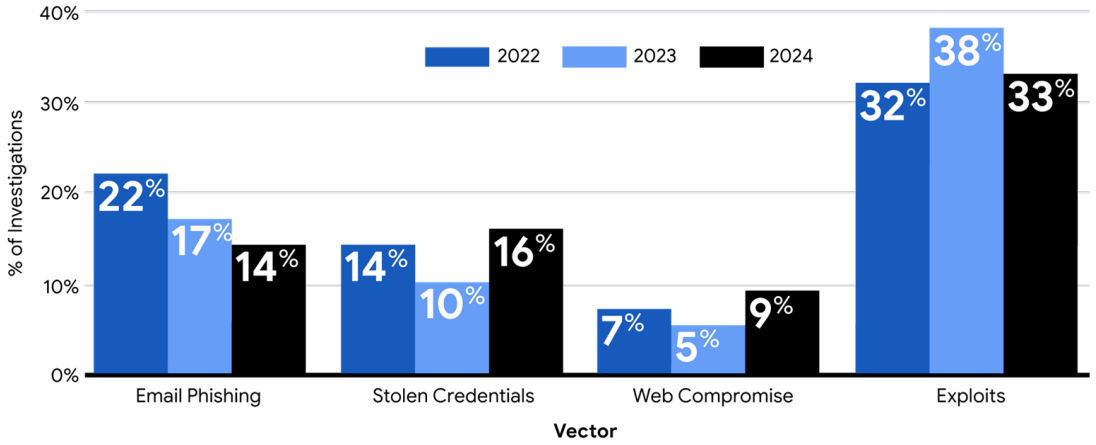
How attackers do it

Infection vectors and attacker techniques

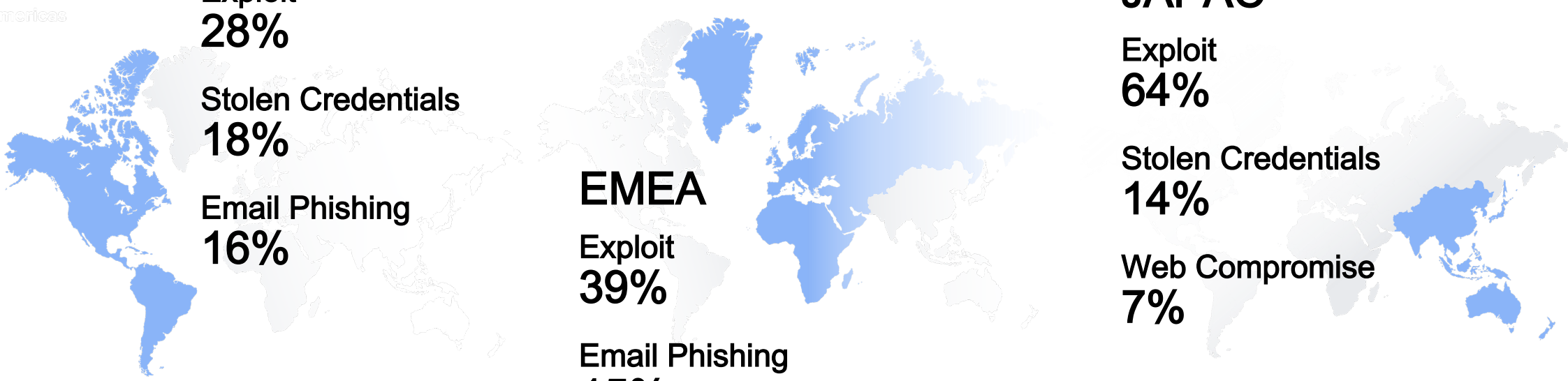
Initial Infection Vector

The continued prevalence of phishing and credential theft underscores the importance of implementing MFA, preferably FIDO2-compliant MFA methods.

Phishing Declines as an Initial Infection Vector, 2022 -2024



Initial Infection Vector – By Region



AMERICAS

Exploit
28%

Stolen Credentials
18%

Email Phishing
16%

EMEA

Exploit
39%

Email Phishing
15%

Brute Force
10%

JAPAC

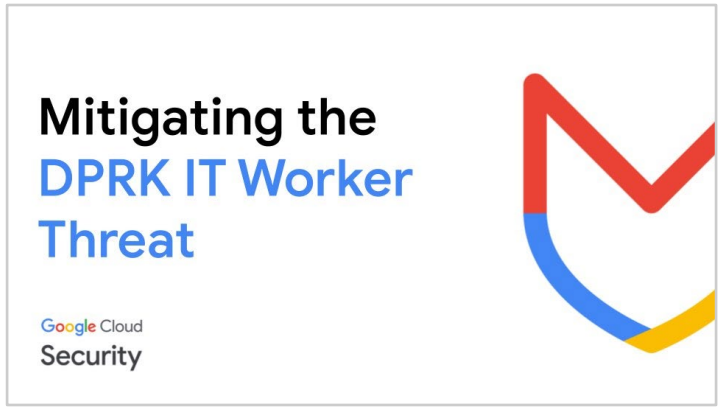
Exploit
64%

Stolen Credentials
14%

Web Compromise
7%

Post Compromise Activity
Insider Threat

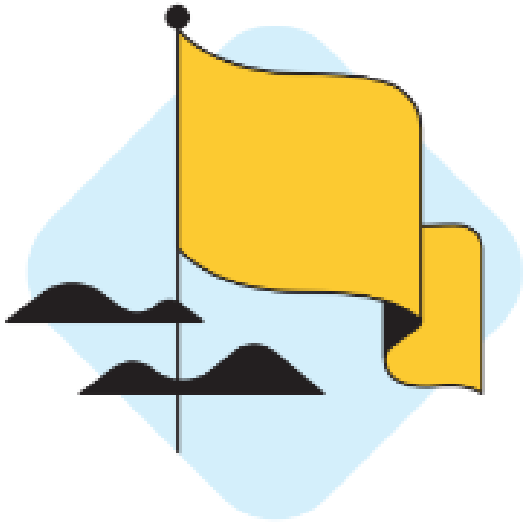
- North Korean IT workers tracked as as UNC5267
- Gain elevated access to modify code and administer network systems
- Demand ransom after stealing proprietary data
- Staying a Step Ahead: Mitigating the DPRK IT Worker Threat.11



Adversaries Use of Gemini

Key Findings

- Attackers use Gemini as another **productivity tool**
- We did not observe threat actors using **novel or unique** AI-enabled attack or abuse techniques
- **Gemini's safety measures** continue to **restrict** adversarial operational capabilities
- We did not observe attempts by threat actors to use prompt attacks or other ML-focused threats as outlined in the Secure AI Framework (SAIF) risk taxonomy

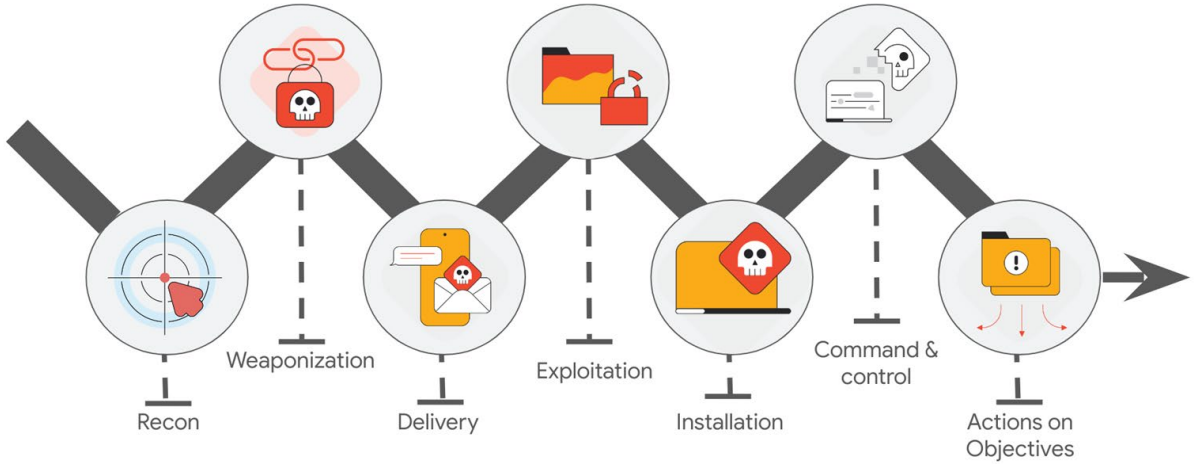


Use of Gemini in APT campaigns

Gemini use across the attack lifecycle.

Use cases include:

- Reconnaissance
- Vulnerability research
- Phishing/social engineering text creation
- Scripting/coding (including payload development)



RSAC 2025 Conference

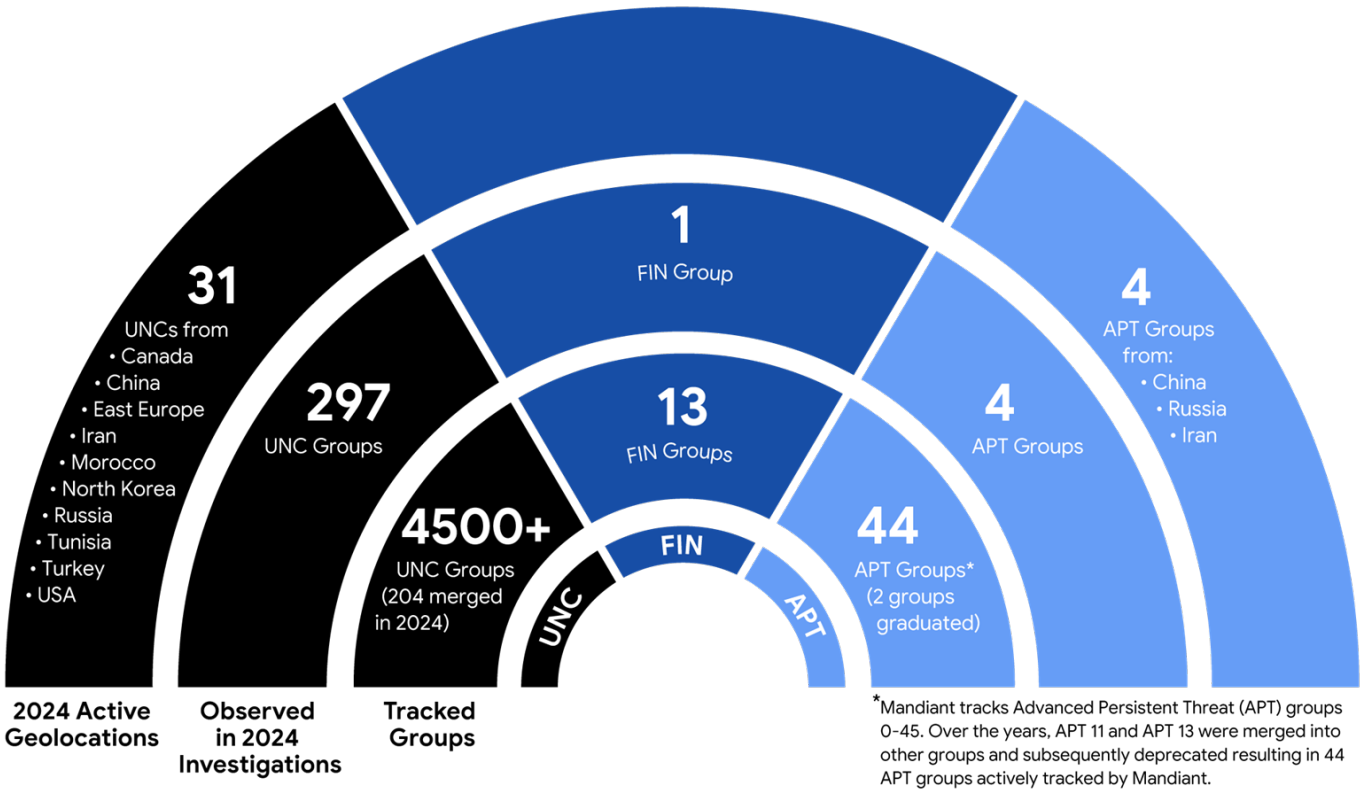
Many Voices. One Community.

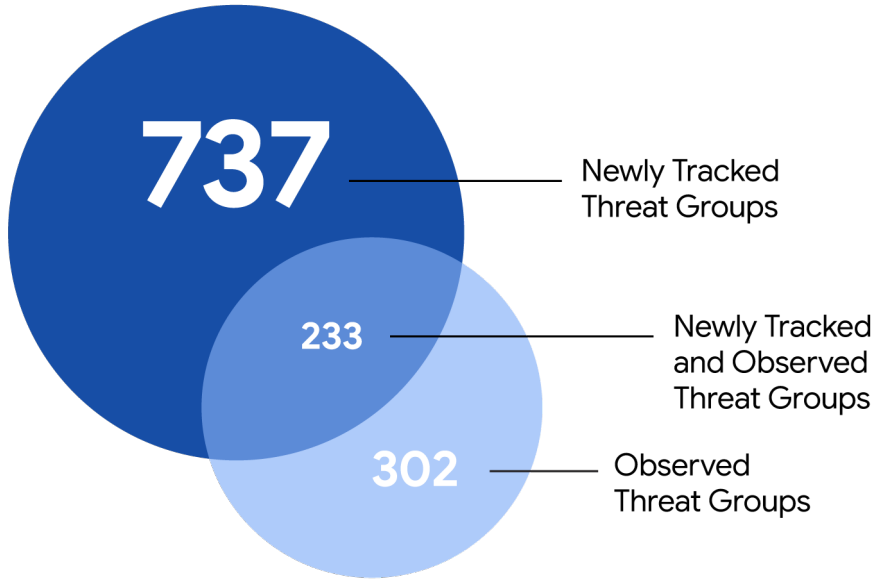
Who attackers are

Threat groups and malware families

2024 Threat Groups

The most frequently observed attackers in the Americas were UNC5267 UNC5221 and UNC2565.

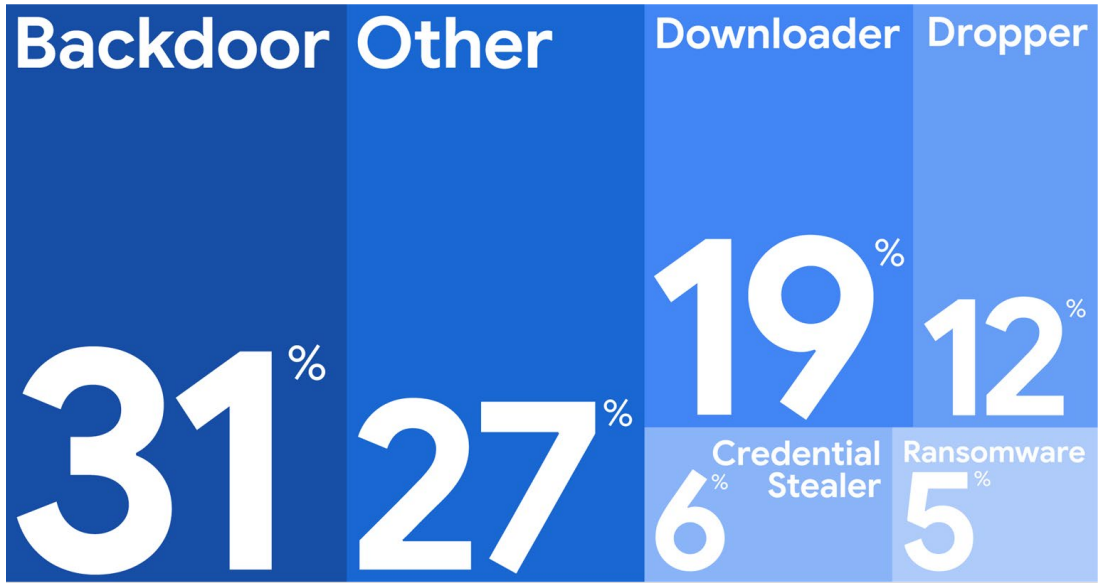




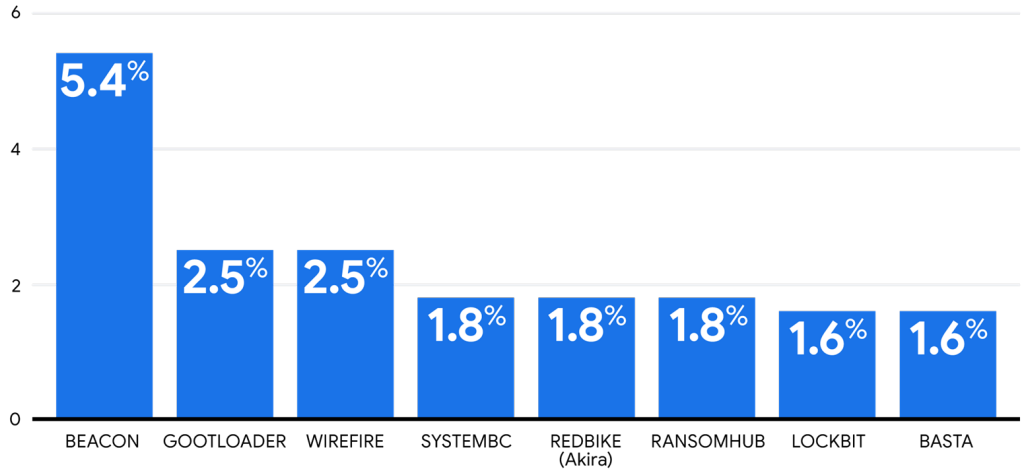
Malware Families

For the fifth consecutive year, BEACON was identified as the most frequently observed malware family in Mandiant investigations globally

Observed Malware Families by Category, 2024



Most Frequently Seen Malware Families, 2024



Graduations

APT44's support of the Kremlin's political objectives has resulted in some of the largest and most consequential cyber attacks in history.

The group is known for:

- First-of-their-kind disruptions of Ukraine's energy grid
- Nearly all of the disruptive and destructive operations against Ukraine over the past decade
- Aggressively using network attack capabilities across political and military contexts

APT45 has carried out a range of cyber operations aligned with the shifting geopolitical interests of the North Korean state.

Activities include:

- Espionage campaigns against government agencies and defense
- Financially-motivated operations, including targeting of the financial vertical
- Executing one of the few publicly known instances of North Korean cyber operations targeting critical infrastructure.

RSAC 2025 Conference

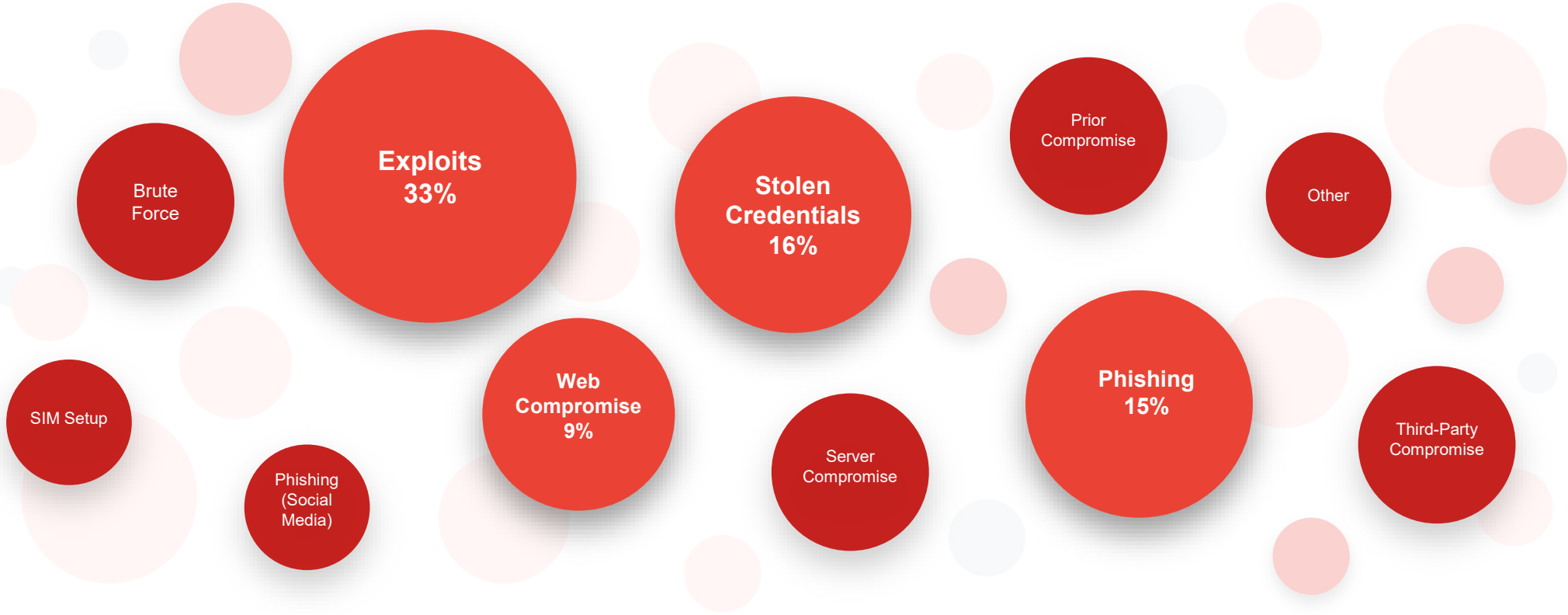
Many Voices.
One Community.

Protecting customers

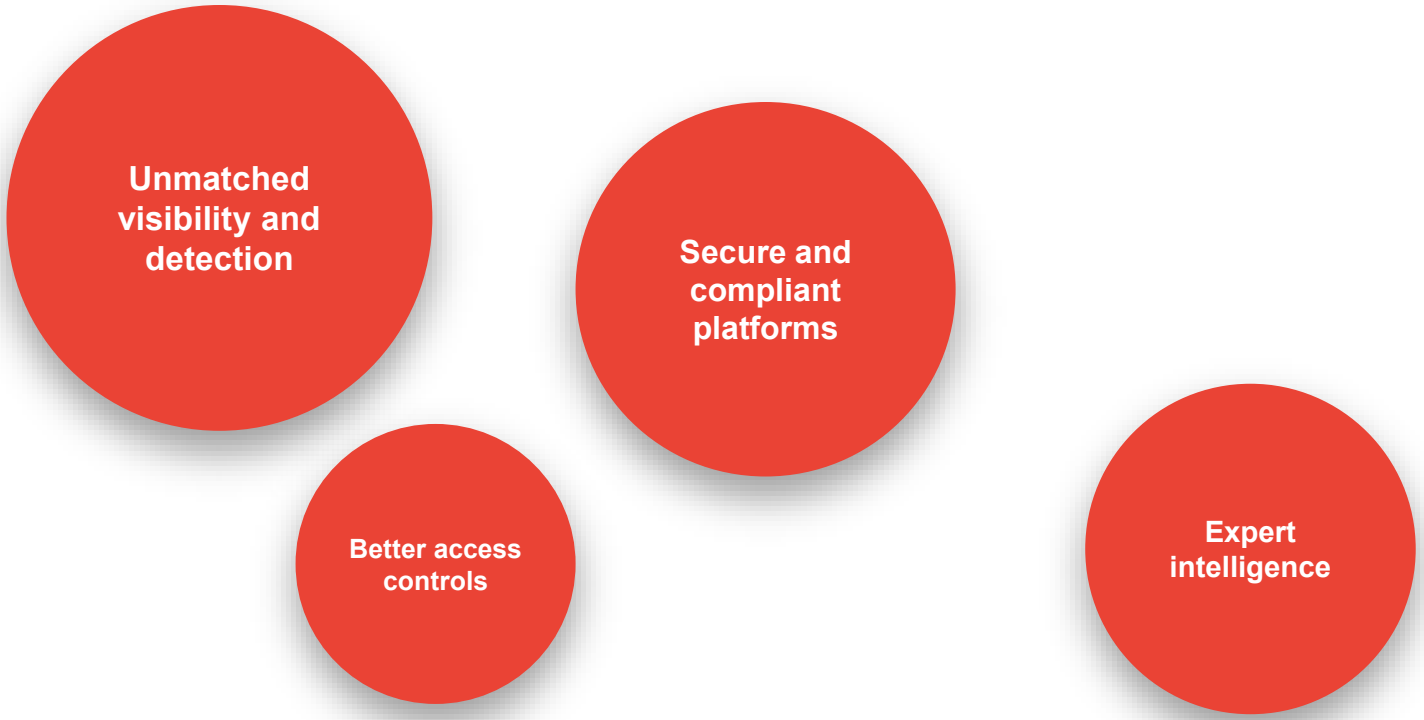
Threat actors are bypassing traditional security controls

The most common initial infection vectors are exploits, phishing, and stolen credentials.

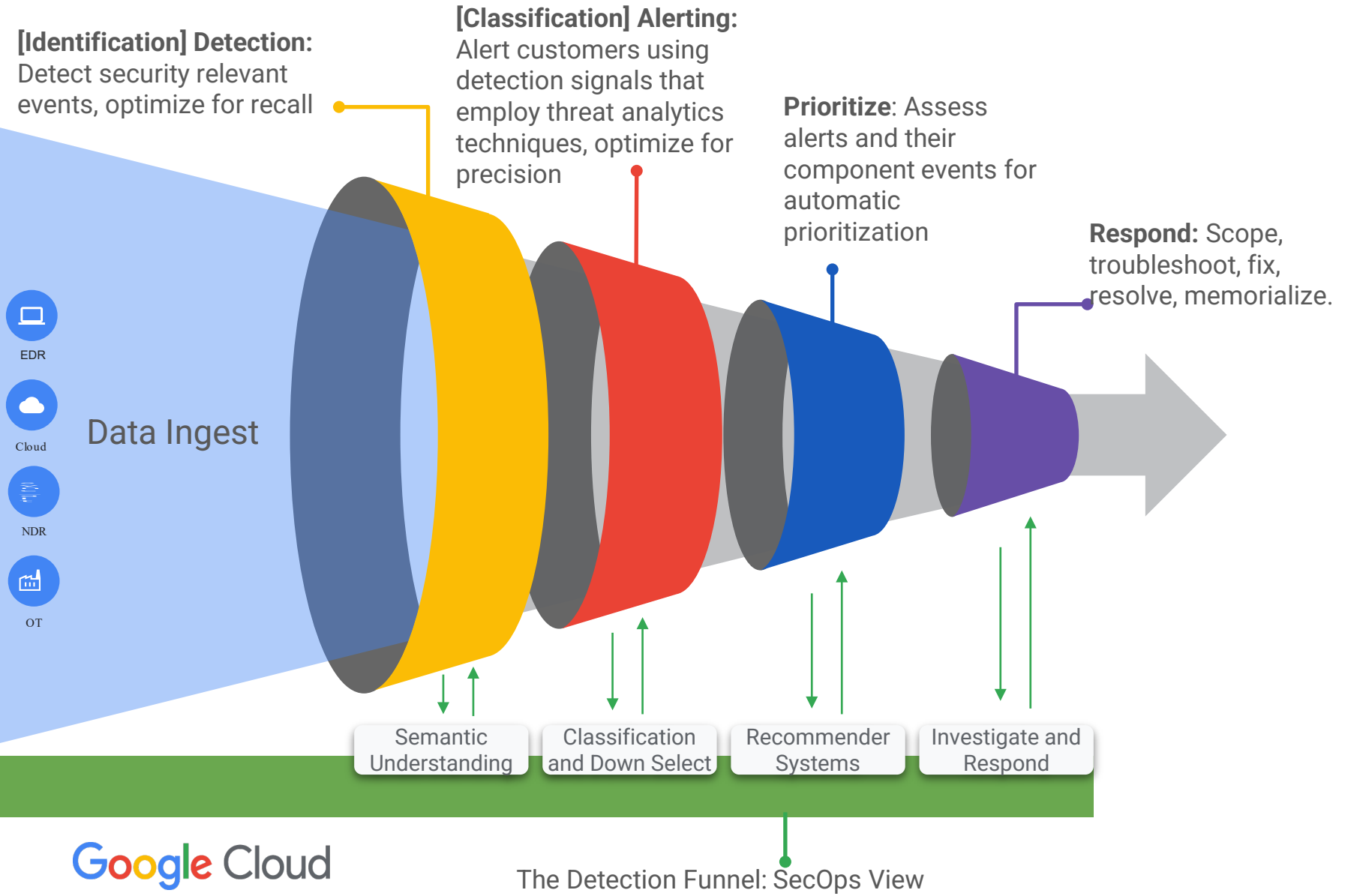
M-Trends 2025 top attack trends:



How can you stop them?



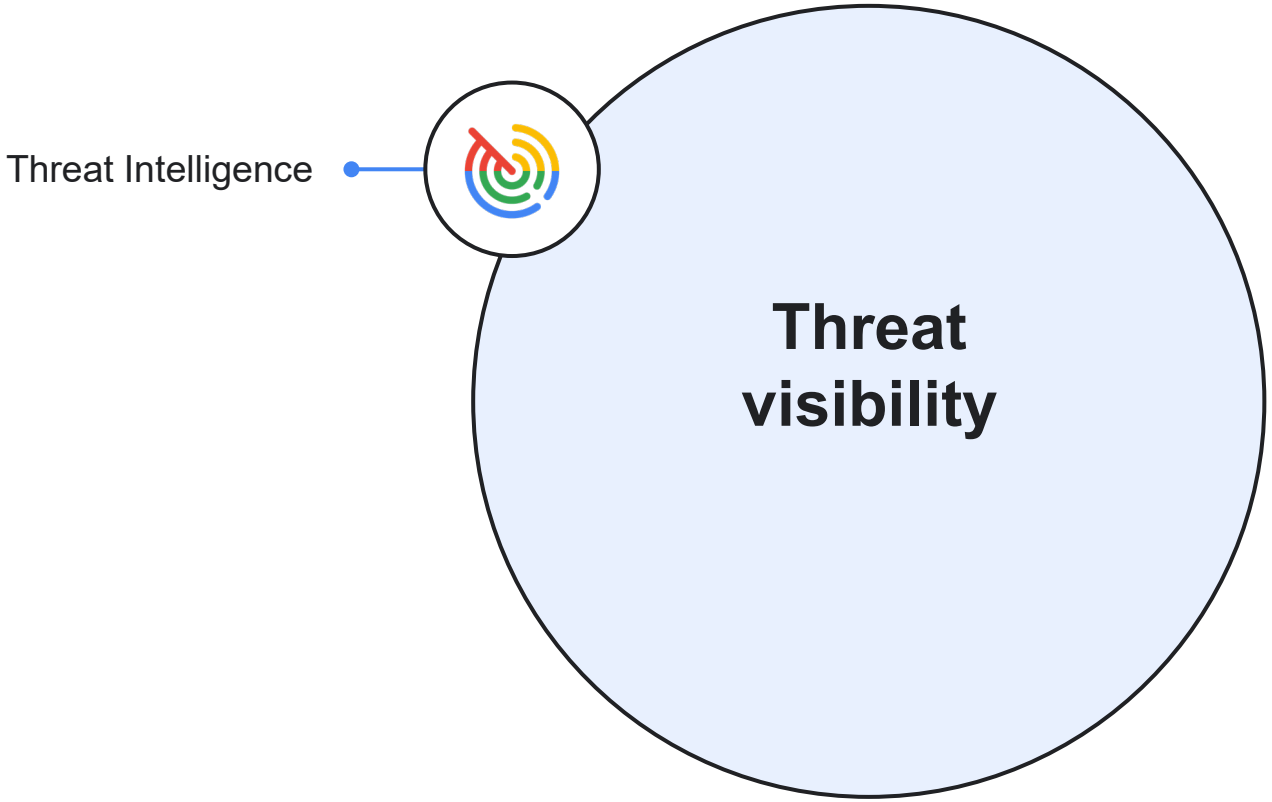
A New Detection Funnel



Desired Outcomes:

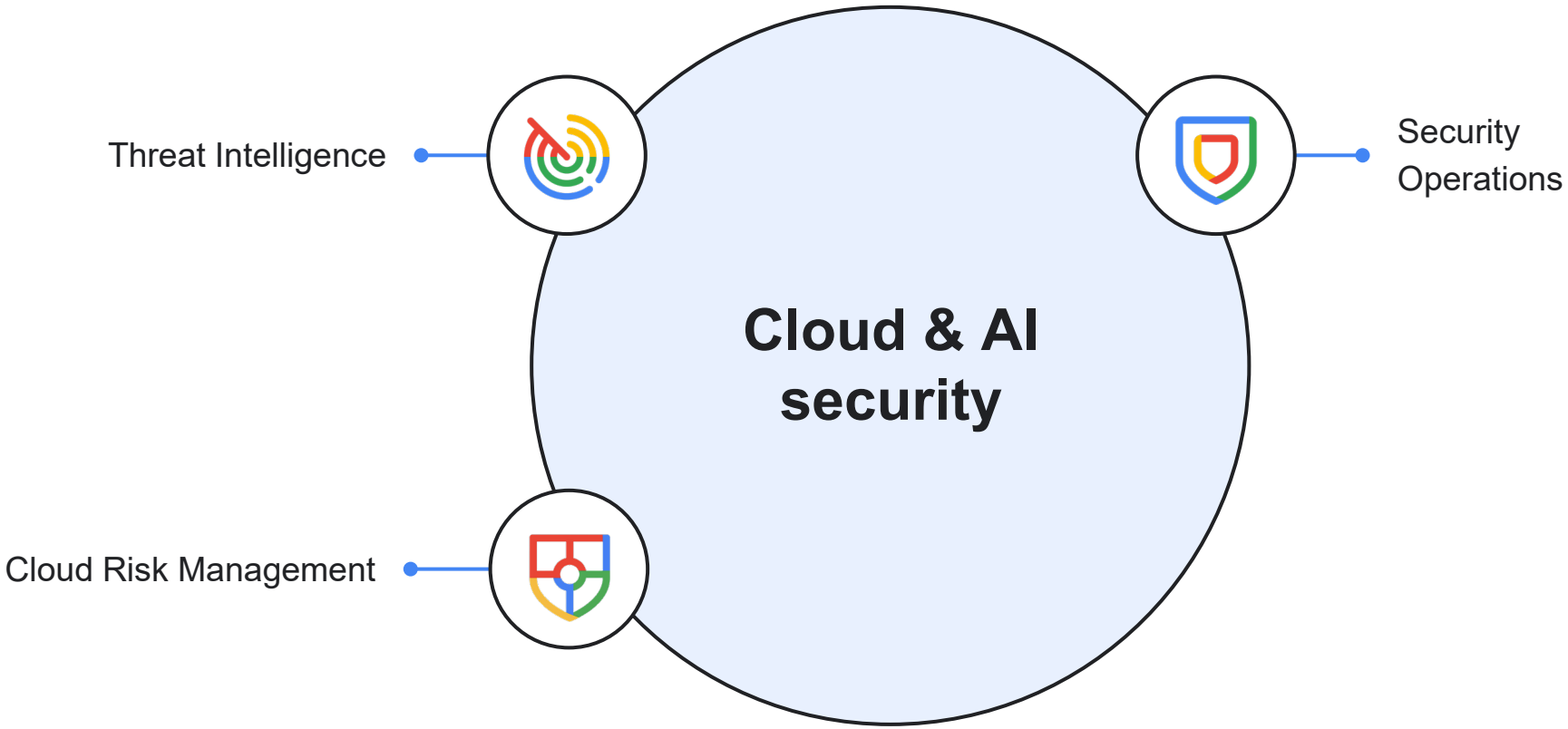
- Maximize threat detection (**recall**) with broad identification.
- Minimize alert noise (**precision**) with composite classification.
- Enable faster incident triage with high-fidelity alerts.
- Build a base for future alert prioritization and advanced detection techniques.

Security requirements

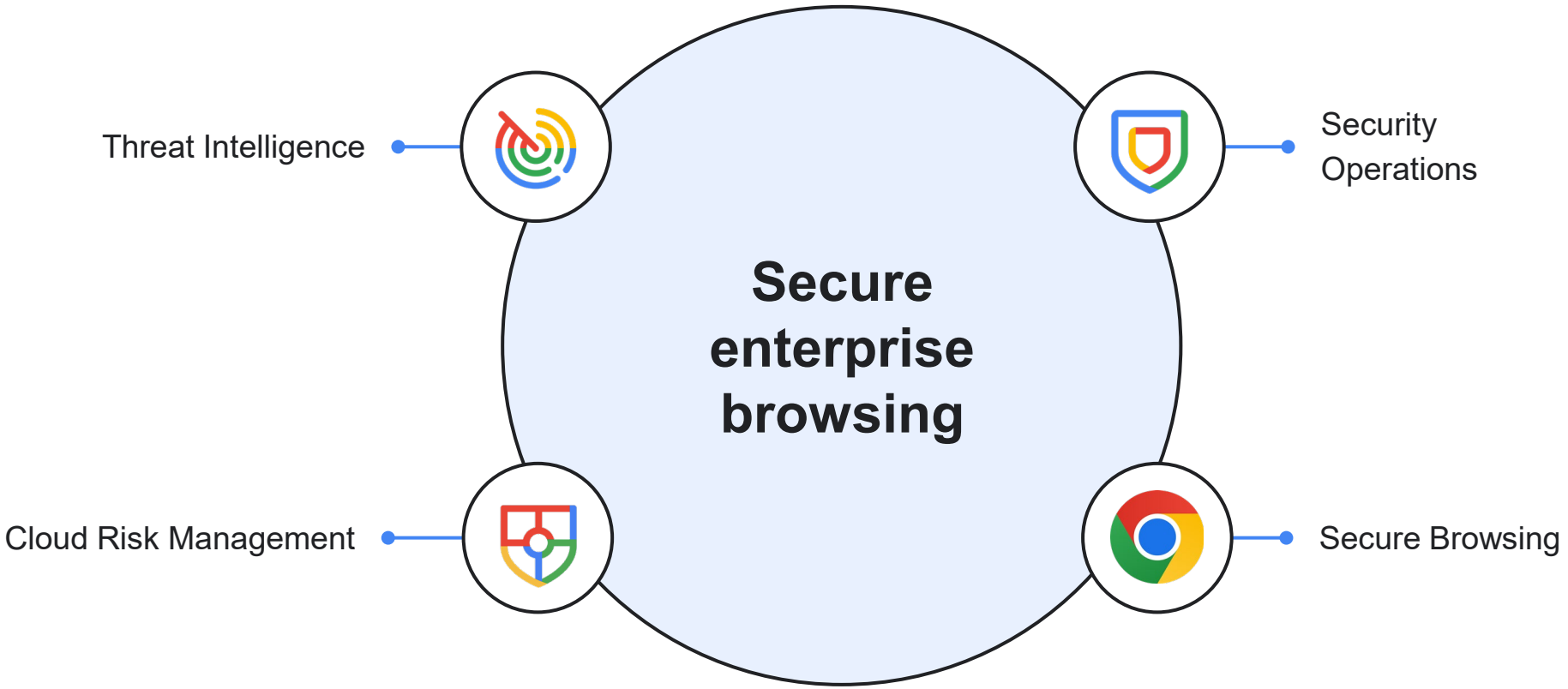


Security requirements

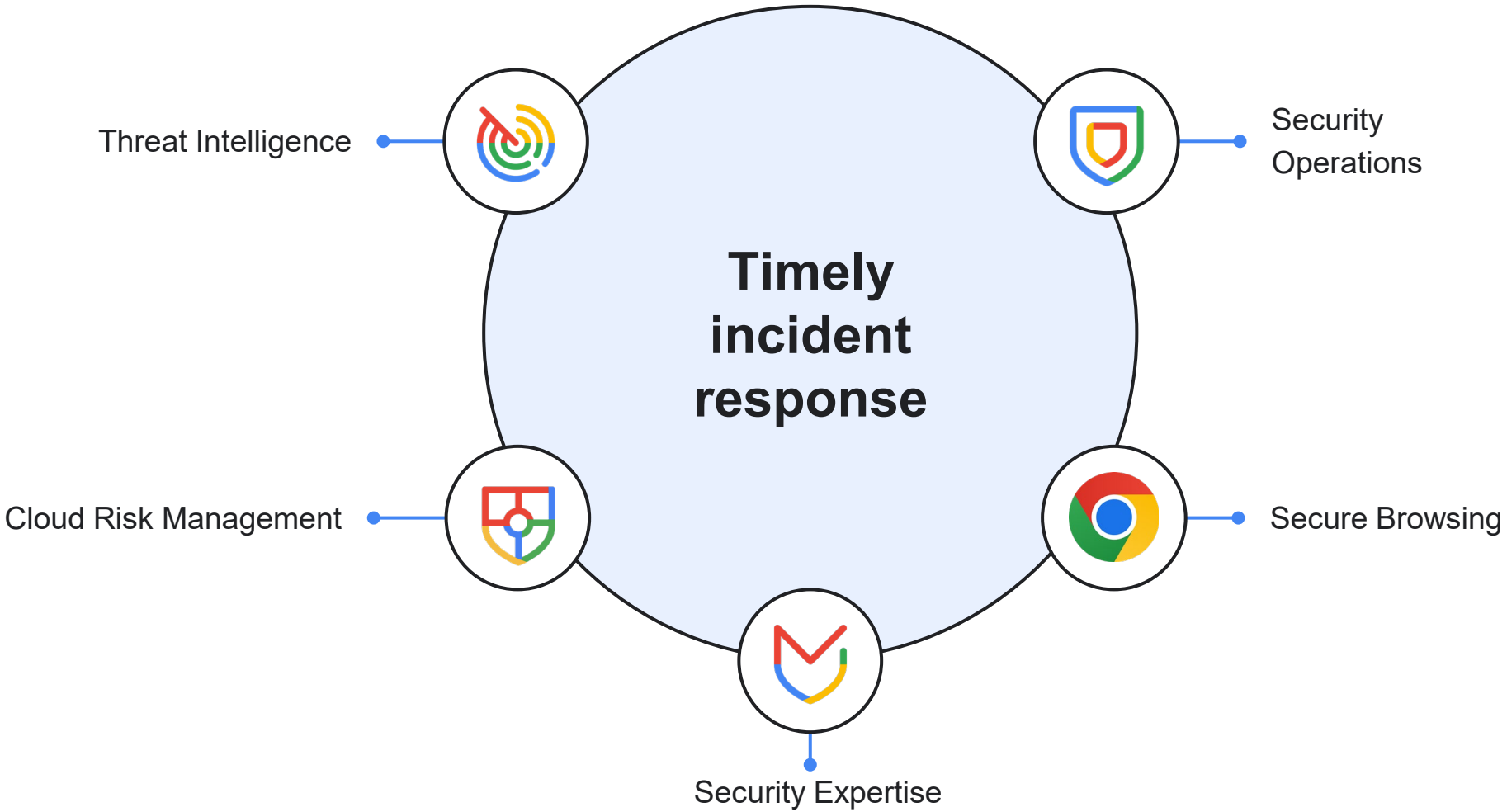
Security requirements



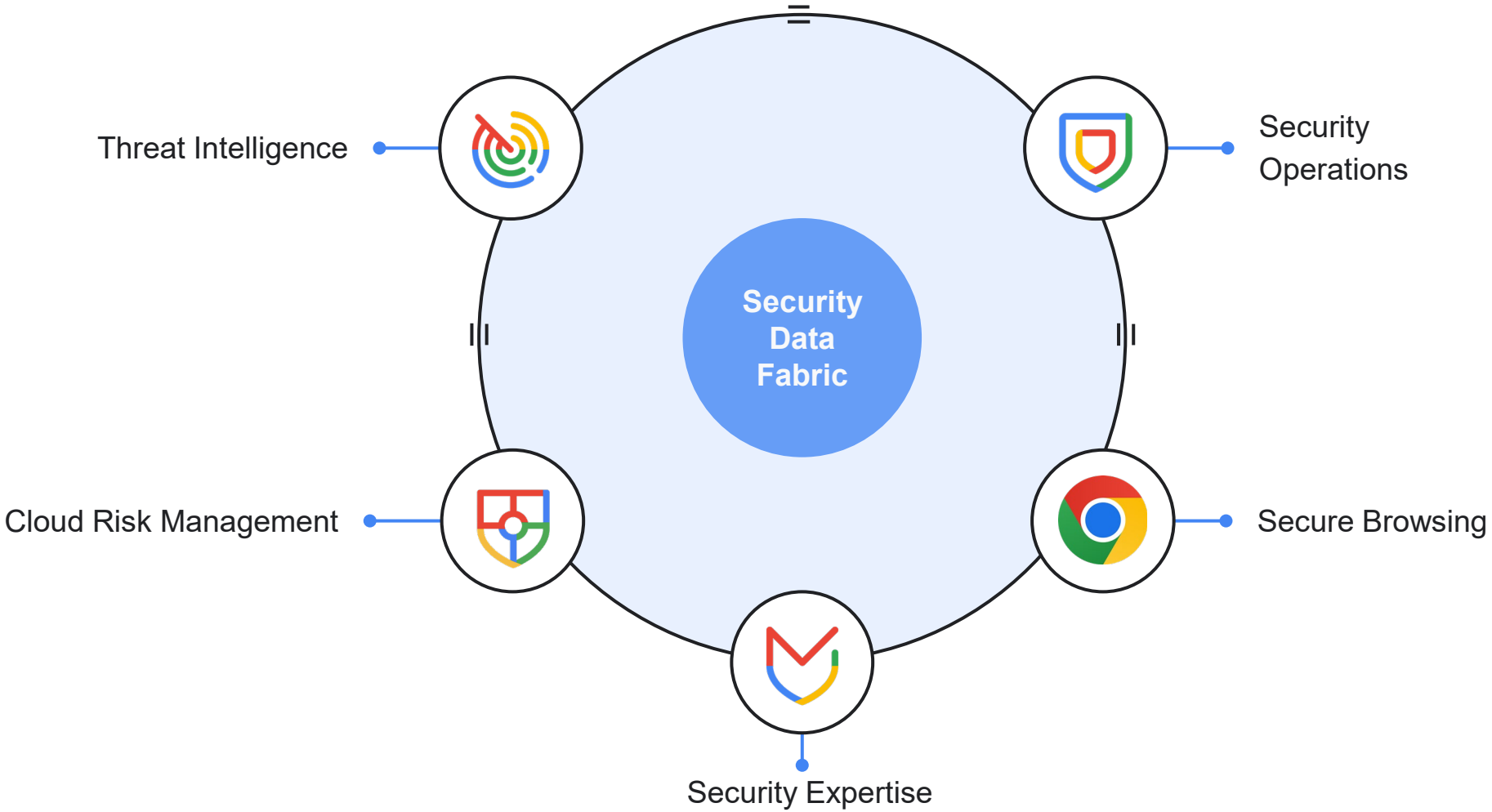
Security requirements



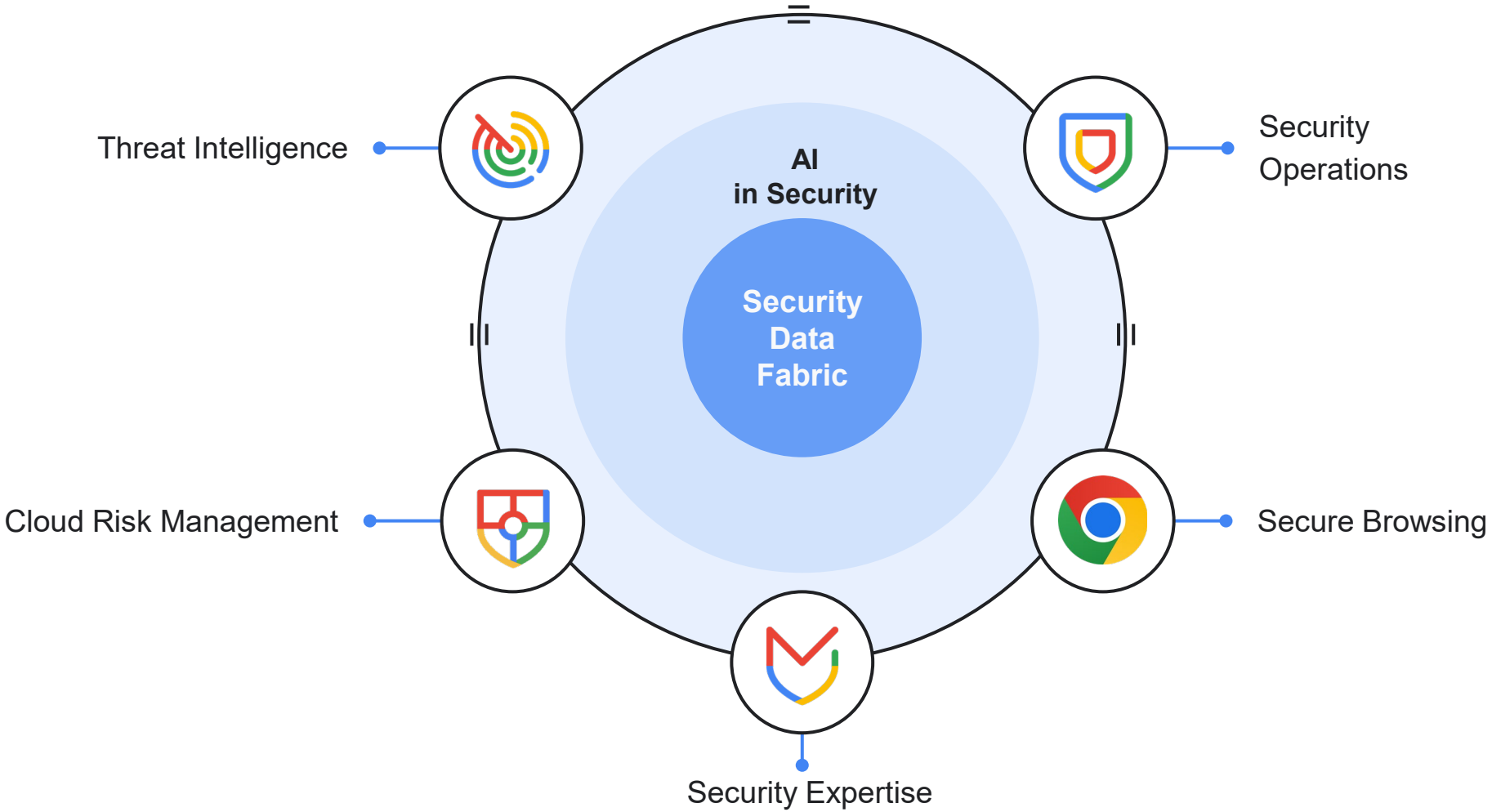
Security requirements



Security requirements



Security requirements



Introducing 2025 M -Trends Rule Packs

Proactively uncover and defend against the latest threats

Leverage rule packs released for specific M-trends 2025 trends

Easily detect infostealer malware, cloud compromise and data theft

```
rule composite_mtrends_infostealer {

  customer_meta:
    rule_name = "Composite: Mtrends Infostealer"
    description = "Composite rule to look for multiple infostealer base detections for a host"
    severity = "High"
    reference = "mtrends infostealer report"

  events:
    $d.detection.detection.rule_name = /base_infostealer/ nocase
    $hostname = $d.detection.detection.outcomes["victim_name"]

  match:
    $hostname over 24h

  outcome:
    $rule_count = count_distinct($d.detection.detection.rule_name)
    $risk_score = (40 + $rule_count * 10)
    $rule_names = array_distinct($d.detection.detection.rule_name)

  condition:
    $d and $rule_count >= 3
}
```

Applying Preemptive Strategies in your Organization

- ➔ Deploy and optimize advanced threat detection technologies
- ➔ Regularly scan for vulnerabilities
- ➔ Strengthen access controls
- ➔ Develop and regularly test incident response and recovery plans
- ➔ Engage red teams to test defenses
- ➔ Invest in ongoing security awareness training and phishing simulations

Welcome to the

Google Cloud Security Community

Here's where you'll find a buzzing community of Security professionals from around the world with one common mission: bringing their Security platforms to the next level.

Search

[Get the latest](#) **insights from Mandiant**

See it in action
Booth N-6062

Join the community

RSAC™ | 2025 Conference

Thank you!